AO 106 (Rev. 04/10) Application for a Search Warrant AUSA Glenn-Applegate

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

A certain cellular phone seized during the arrest of Mohamed Toure on July 26, 2021

Case No. 2:21-mj-511

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment F

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 1956	Money Laundering
18 USC 1957	Money Laundering
18 USC 1343	Wire Fraud

The application is based on these facts:

See attached affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Shawn Mincks, Special Agent, IRS-CI
Printed name and title

Sworn to before me and signed in my presence.

Date: 8/2/2021

Judge's signature

City and state: Columbus, OH

Elizabeth A. Preston Deavers, U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

AFFIDAVIT
IN SUPPORT OF SEARCH WARRANTS

I, Shawn Mincks, Special Agent, U.S. Department of the Treasury, Internal Revenue Service, Criminal Investigation (IRS-CI), being duly sworn, depose and say that:

Introduction and Purpose

1. I am a Special Agent with IRS-CI and have been so employed since 2008. I have received specialized law enforcement training at the Federal Law Enforcement Training Center, Glynco, Georgia and additional specialized training from the IRS. My duties as a Special Agent include conducting investigations of individuals and businesses that have violated Federal Law, particularly those laws found under Title 18, Title 26 and Title 31 of the United States Code. I have participated in multiple such investigations, including several investigations related to individuals who launder funds derived from romance and other international fraud schemes.

2. I am assigned to pursue a federal criminal investigation of Robert Asante (Asante), Alexis Wellington (Wellington), Mohamed Toure (Toure), Uriah Lamdul (Lamdul), Edward Amankwah (Amankwah) and other co-conspirators. I make this affidavit in support of search warrants for cellular phones seized by IRS-Criminal Investigation during the arrests of Wellington, Toure, Lamdul and Amankwah on July 26, 2021. These items are further described as the following and are also described in Attachments A, B, C and D:

Attachment A

a. Rose Gold iPhone cell phone seized during the execution of an arrest warrant on Alexis Wellington

Attachment B

a. Black and Gray iPhone cell phone seized during the execution of an arrest warrant on Mohamed Toure

Attachment C

a. Black iPhone cell phone seized during the execution of an arrest warrant on Uriah Lamdul

Attachment D

a. Black Samsung cell phone seized during the execution of an arrest warrant on Edward Amankwah

3. These devices are currently in the possession of IRS-CI located at 401 North Front Street, Suite 375, Columbus, Ohio.

4. The information in this affidavit is either personally known to me based upon my experience, investigative activities, analysis of records and interviews; or it has been relayed to me by other agents and/or law enforcement personnel. This affidavit is being submitted for the limited purpose of securing a search warrant, and I have not included each and every fact known to me concerning the investigation. I have set forth only the facts I believe are necessary to support the requested search warrant.

5. I contend there is probable cause to believe that Asante, Wellington, Toure, Lamdul and Amankwah were engaged, together and with others, in a conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h). Additionally, I contend that Asante, Wellington, Toure, Lamdul and Amankwah each personally committed multiple acts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1957; and Asante and Wellington engaged in a conspiracy to commit bank fraud in violation of 18 U.S.C. § 1349. I further contend that evidence of such violations and evidence of wire fraud in violation of 18 U.S.C. § 1343 is located on or in the items described in paragraph #2 and in Attachments A, B, C and D.

Overview of the Scheme

6. From at least October 25, 2018 through the present, Asante, Wellington, Toure, Lamdul and Amankwah conspired together and with others to launder funds derived from romance and other fraud schemes.

7. Perpetrators of the fraud schemes posted fake profiles on various dating or social media websites. Then, individuals throughout the United States and the world were contacted by or enticed to initiate contact with the scammers. After contacting the victims online, the scammers used email, instant messaging services, text messaging, various smart phone applications and phone calls to build a relationship of trust with the victims. Once trust was gained, the scammers convinced the victims to provide money purportedly for investments or need-based reasons. The scammers explained, for example, that they had acquired an inheritance and needed assistance with transporting the assets; had financial trouble and needed assistance; or had had legal trouble. The scammers then contacted Asante directly or contacted a money broker in Ghana, who contacted Asante. Asante provided the scammers or money broker with routing and account numbers for bank accounts opened by individuals he recruited in the United States to accept funds derived from the scams. The bank account holders Asante recruited included Wellington, Toure, Lamdul and Amankwah. The scammers then instructed the victims to send funds to the bank accounts as arranged by Asante. The victims then mailed checks to the account holders and/or wire transferred, direct transferred or deposited money into the bank accounts. Evidence indicates that many of these bank accounts were opened in the names of business entities established by Wellington, Toure, Lamdul and Amankwah. The victims provided the funds with the expectation that the money would be invested or used to assist their online "friend."

8. Contemporaneous with and subsequent to the wire transfers, account transfers and deposits received from the victims, Wellington, Toure, Lamdul and Amankwah disposed of the funds through cash withdrawals; checks issued to and transfers to bank accounts held by third-parties; international and domestic wire transfers; personal expenditures; and purchases of official checks.

9. Additionally, Toure received into a bank account under his control proceeds of a fraudulent Economic Injury Disaster Loan (EIDL) in the amount of $109,900. After receiving the funds, he conducted transactions designed to conceal the nature, source, location, control and ownership of the funds.

10. On June 23, 2020, a federal grand jury returned an indictment charging Asante and two others with one count each in violation of 18 U.S.C. § 1956(h) for their roles in the money laundering conspiracy. The two others have since entered guilty pleas to the charges.

11. On July 8, 2021, a federal grand jury returned a superseding indictment charging Asante, Wellington, Toure, Lamdul and Amankwah each with one count in violation of 18 U.S.C. § 1956(h) and multiple counts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and 18 U.S.C. § 1957. One of the § 1956(a)(1)(B)(i) counts for Toure was related to laundering the proceeds of the EIDL. Asante and Wellington were also charged with one count in violation of 18 U.S.C. § 1349, Conspiracy to Commit Bank Fraud.

12. On July 26, 2021, Wellington was arrested by IRS-CI Special Agents at her home located at 6420 Rossi Drive, Canal Winchester, OH. During the arrest, IRS-CI Special Agents escorted Wellington into her bedroom to dress prior to being transported to the United States Marshals Service for processing. In the bedroom, IRS-CI Special Agents told Wellington she would need to call somebody later that day if she was released from custody. Wellington identified a Rose Gold iPhone cell phone located on the bed as hers. IRS-CI Special Agents seized the phone in order to preserve evidence on the phone pending application of a search warrant by the affiant.

13. On July 26, 2021, Toure was arrested by IRS-CI Special Agents at his home located at 1863 Mintwood Drive, Columbus, OH. The only other occupant of the residence was a female. During the arrest, IRS-CI Special Agents escorted Toure into his bedroom to dress prior to being transported to the United States Marshals Service for processing. In the bedroom, IRS-CI Special Agents saw a Black and Gray iPhone cell phone located on the bed. IRS-CI Special Agents asked Toure if the phone was his and if he would like to take it with him. Toure replied in the affirmative. Toure identified a second phone in the bedroom as belonging to the female. IRS-CI Special Agents seized Toure's phone in order to preserve evidence on the phone pending application of a search warrant by the affiant.

14. On July 26, 2021, Lamdul was arrested by IRS-CI Special Agents at his employer located at 6405 Commerce Court, Groveport, OH. When searched incident to arrest, IRS-CI Special Agents discovered that Lamdul had a Black iPhone cell phone on his person in the pocket of his shorts. IRS-CI Special Agents seized the phone in order to preserve evidence on the phone pending application of a search warrant by the affiant.

15. On July 26, 2021, Amankwah was arrested by IRS-CI Special Agents at his home located at 5390 Cambria Drive, Westerville, OH. Amankwah was the only occupant of the residence. During a security sweep of the home, IRS-CI Special Agents saw a black Samsung cell phone on a table. As Amankwah was being searched incident to arrest, he indicated that the black Samsung cell phone on the table was his. IRS-CI agents seized the cell phone to preserve evidence on the phone pending application of a search warrant by the affiant.

Summary of Bank Accounts and Entities

16. According to records from the Ohio Secretary of State, on September 14, 2018, Wellington established Lexis Solutions Group, LLC (LSG) by filing Articles of Organization. Wellington did so through National Filing Systems, LLC, a third-party assisted filing service. According to bank records, Wellington then opened and controlled the following bank accounts in the name of LSG and was the only signer on each account:

a. October 10, 2018 – November 9, 2018: Bank of America account # xx4736 (BOA xx4736).

b. November 1, 2018 – December 31, 2018: JP Morgan Chase Bank account # xx3056 (JPMC xx3056).

17. According to records from the Ohio Secretary of State, on June 19, 2019, Toure established Lamzol Trucking & Logistics, LLC (Lamzol) by filing Articles of Organization. Toure also did so through National Filing Systems. According to bank records, Toure then opened and controlled the following bank accounts in the name of Lamzol and was the only signer on each account:

a. July 5, 2019 – April 30, 2020 (last available records): Fifth Third Bank account # xx8474.

b. August 8, 2019 – April 30, 2020: Bank of America account # xx1870 (BOA xx1870).

c. January 23, 2020 – September 30, 2020: Key Bank account # xx7237 (KEY xx7237).

18. According to records from the Ohio Secretary of State, on May 30, 2019, Lamdul established Brandtown Logistics, LLC (Brandtown) by filing Articles of Organization. Lamdul also did so through National Filing Systems. According to bank records, Lamdul then opened and controlled the following bank accounts in the name of Brandtown and was the only signer on each account:

a. June 12, 2019 – November 6, 2019: JP Morgan Chase Bank account # xx9579 (JPMC xx9579).

b. November 21, 2019 – February 29, 2020: Bank of America account # xx3392 (BOA xx3392).

c. February 3, 2020 – May 5, 2020: Key Bank account # xx7278 (KEY xx7278).

19. According to records from the Ohio Secretary of State, Amankwah established EKA Consulting, LLC (EKA) on October 17, 2016 by filing Articles of Organization. According to bank records, Amankwah opened and controlled the following bank accounts in the name of EKA and was the only signer on each account:

a. July 22, 2019 – March 31, 2020: JP Morgan Chase Bank account # xx7723 (JPMC xx7723).

b. July 11, 2018 – June 5, 2020: PNC Bank account # xx4725 (PNC xx4725).

c. October 4, 2019 – March 31, 2020: Bank of America account # xx2925 (BOA xx2925).

Evidence of Probable Cause

Wellington and Lexis Solutions Group (LSG)

20. According to an interview with Person 23's husband, whose identity is known to the affiant, Person 23 was scammed by somebody he/she met on Facebook. The person he/she met eventually told Person 23 that he needed help getting a box of valuables back into the United States. The money Person 23 sent at this person's direction was supposed to pay for customs and other fees. The valuables never made it to the United States, and the person always needed more and more money. Person 23 eventually reported the incident to the FBI. Bank records show that, on October 25, 2018, Person 23 wired $275,000 to BOA xx4736.

a. Bank records show that, after receiving these funds and on or about the date set forth below, Wellington engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

i. October 29, 2018 - $242,000 wire to a company in Ghana.

21. Bank records show that deposits into BOA xx4736 between October 10, 2018 and November 9, 2018 totaled $292,550, excluding the redeposit of a check issued from the account. Of these deposits, at least $275,000 was derived from romance fraud.

22. According to an interview with Person 37, whose identity is known to the affiant, Person 37 met somebody he/she believed to be named James Lawson on a dating website. Lawson told Person 37 that he was in Syria working for a private company and had found gold. The gold had been divided amongst the owners of the company. Lawson and somebody Person 37 believed to be named Agent Dillon instructed Person 37 to send money to various companies to pay for license and other fees related to the gold. Person 37 stated that he/she filed an Internet Crime

Complaint Center (IC3) report with the FBI about this incident. Bank records show that, on November 23, 2018, Person 37 transferred $272,000 into JPMC xx3056. After the funds were received into JPMC xx3056, JP Morgan Chase Bank froze the account.

23. Bank records show that deposits into JPMC xx3056 between November 1, 2018 and January 2, 2019 totaled $301,449.05. This total included $29,149.05 from the closure of BOA xx4736 and $272,000 from Person 37.

24. On January 2, 2019, JP Morgan Chase disbursed the previously frozen funds to Wellington through the issuance of an official check in the amount of $272,000 and closed JPMC xx3056. On January 25, 2019, Wellington opened PNC Bank account # xx9694 (PNC xx9694) in the name of LSG and was the only signer on the account. On that same date, she deposited the official check issued by JP Morgan Chase Bank into PNC xx9694. After depositing the funds into PNC xx9694, and on or about the date set forth below, Wellington engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

a. February 28, 2019 – issuance of a check in the amount of $221,200 to Company 5.

Toure and Lamzol Trucking and Logistics (Lamzol)

25. According to an interview with Person 38, whose identity is known to the affiant, he/she met several people on Facebook and has fallen victim to more than one scam. The scammers told Person 38 they were in the military and asked him/her to assist them by sending money to them. The money was supposed to be used to help them get home or to pay transportation fees related to gold. Person 38 fell victim to two or three of these scams before he/she learned his/her lesson. Person 38 was never reimbursed and never received any gold.

a. Bank records show that, on August 5, 2019, a check issued to Lamzol by Person 38 in the amount of $47,325 was deposited into FTB xx8474. Bank records show that, after receiving the funds and on or about the dates set forth below, Toure engaged in the following monetary transactions in criminally derived property of a value greater than $10,000, which were also financial transactions designed to conceal the nature, source, location, ownership and/or control of the funds:

i. August 16, 2019 – purchase of an official check in the amount of $41,646 payable to himself.

ii. August 19, 2019 – deposit of official check in the amount of $41,646 into BOA xx1870.

iii. August 27, 2019 – wire in the amount of $41,500 from BOA xx1870 to Company 11. A memo on the wire read, "Employee compensation."

26. According to an interview with Person 39, whose identity is known to the affiant, Person 39 met somebody he/she believed to be named Brenda Tincher on a dating website in 2019. Tincher told Person 39 that she had inherited gold from her father's estate and needed assistance in paying fees related to the gold. The gold was supposed to be shipped to Person 39's home, but he/she did not receive any gold. Bank records show that, on December 9, 2019 and December 16, 2019, Person 39 wired $28,200 and $35,780, respectively, to BOA xx1870.

a. Bank records show that, after receiving the funds, Toure engaged in the following monetary transactions in criminally derived property of a value greater than $10,000, which were also financial transactions designed to conceal the nature, source, location, ownership and/or control of the funds:

i. December 10, 2019 - $20,000 wire to Conspirator 14

ii. December 17, 2019 - $20,000 wire to Conspirator 15

iii. December 17, 2019 - $11,000 transfer to Company 12

27. According to an interview with Person 40, whose identity is known to the affiant, Person 40 believed he/she was in an online relationship with somebody named David Wayne. Wayne told Person 40 that he was a diplomat in Denmark. Wayne told Person 40 that he needed money to invest in gold exports from Africa. Person 40 sent over $500,000 to individuals and companies at Wayne's direction. Person 40 eventually realized he/she was the victim of a scam. Bank records show that, on December 18, 2019, $22,500 from Person 40 was deposited into BOA xx1870.

28. According to an interview with Person 41, whose identity is known to the affiant, Person 41 began communicating with somebody he/she believed to be named Julius Smith Fuseini in 2016. Fuseini told Person 41 that he needed assistance with a shipment of diamonds and gold located in Ghana. Since that time, Person 41 has communicated with what he/she believed to be several other individuals. The group has instructed Person 41 to send funds to various people and places to facilitate the transport of the gold and diamonds. Person 41 estimates he/she has sent more than $3 million in relation to communications with the Fuseini group. Person 41 has not received any gold or diamonds. Bank records show that, on December 19, 2019, Person 41 wired $400,000 to BOA xx1870. These funds were returned to Person 41 by Bank of America.

29. On July 15, 2020, Key xx7237 received an ACH deposit from the SBA in the amount of $109,900. Information related to the ACH shows that it pertained to loan # 2236148101.

a. SBA documents show that loan # 2236148101 was an EIDL issued to a company named (Person 45) Medical Equipment, LLC, allegedly owned by Person 45. The loan applicant entered Person 45's Social Security Number, date of birth and home address. The loan applicant eventually provided information for Key xx7237 as the account to which the loan proceeds were to be paid.

30. According to an interview with Person 45, whose identity is known to the affiant, he/she does not own a company named (Person 45) Medical Equipment and did not apply for an EIDL.

Person 45 does not know Toure and does not know anything about a Key Bank account. Person 45 does not know anything at all about the loan and did not give anyone permission to apply for the loan.

31. After receiving the funds and on or about the date set forth below, Toure engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

a. July 16, 2020 - Withdrawal totaling $28,000 consisting of the purchases of two official checks in the amount of $9,500 each and $9,000 in cash.

32. Further analysis of the bank records related to the accounts held in the name of Lamzol shows that additional funds characteristic of derivation from fraud were deposited and/or wired into the accounts. Not all the individuals from whom funds were received were interviewed. However, deposits from many of the individuals share characteristics with those deposits known to have originated from romance fraud. Deposits into Toure's accounts which were characteristic of fraud totaled at least $951,380.

Lamdul and Brandtown Logistics, LLC (Brandtown)

33. According to an interview with Person 31, whose identity is known to the affiant, Person 31 met somebody he/she believed to be named Michael McNair on a dating website. McNair was too young for Person 31, so he referred Person 31 to Jason LNU. Person 31 and Jason LNU communicated via Google Hangouts. Jason LNU told Person 31 he had a lot of gold and needed to ship the gold to the United States. Jason LNU convinced Person 31 to send money to pay fees and taxes related to the gold. Jason LNU "abandoned" Person 31 when he/she told him he/she could not send any more money. Bank records show that, on September 12, 2019, Person 31 deposited $27,000 cash into JPMC xx9579.

a. Bank records show that, after receiving the funds, Lamdul engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

i. September 16, 2019 - $23,800 wire to Conspirator 12.

34. According to an interview with Person 32, whose identity is known to the affiant, Person 32 met somebody he/she believed to be named Leticia Miles through someone he/she believed to be a business associate located in Holland. Person 32 communicated with Miles via text, phone and email but has never met Miles in person. Miles told Person 32 she needed help with the importation of gold bars. Person 32 sent approximately $400,000 to at least three different companies, including Brandtown. Bank records show that, on September 23, 2019, an official check in the amount of $75,000 purchased by Person 32 was deposited into JPMC xx9579.

a. Bank records show that, after receiving the funds, Lamdul engaged in the

following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

i. September 25, 2019 - $66,000 wire to Company 9 located in Dublin, Ireland. A memorandum on the wire indicated that the wire was for "Ethanol."

35. According to an interview with Person 33, whose identity is known to the affiant, Person 33 met somebody he/she believed to be named Harrison Williams on a dating website in June of 2019. Person 33 communicated with Williams via email and text. Williams told Person 33 that he was an architect who had investments in gold and diamonds located in Dubai. Williams eventually asked Person 33 for money to pay for fees related to the shipment of the gold and diamonds to the United States. Person 33 sent over $200,000 to various recipients, including Brandtown. Bank records show that, on September 27, 2019, Person 33 wired $1,000 and $71,500 into JPMC xx9579.

a. Bank records show that, after receiving the funds, Lamdul engaged in the following monetary transactions in criminally derived property of a value greater than $10,000, which were also financial transactions designed to conceal the nature, source, location, ownership and/or control of the funds:

i. September 30, 2019 - $50,000 wire to a bank account in Canada.

ii. October 4, 2019 - $17,300 wire to Asante.

36. According to an interview with Person 34, whose identity is known to the affiant, Person 34 met somebody he/she believed to be named Robert Michael after Michael contacted him/her on Facebook. They subsequently communicated via Google Hangouts. Michael told Person 34 he was a General in the U.S. military and needed credentials to get home. Michael convinced Person 34 to send approximately $230,000 to various people to assist getting him home. Person 34 mailed a certified check to Brandtown. Bank records show that, on October 29, 2019, an official check in the amount of $58,000 purchased by Person 34 was deposited into JPMC xx9579. A portion of the funds were used by JP Morgan Chase to reimburse another victim. The remaining funds, $22,922.02, were issued to Lamdul when JP Morgan Chase closed JPMC xx9579. Lamdul deposited the check issued by JP Morgan Chase into BOA xx3392.

a. Bank records show that, after depositing the funds into BOA xx3392, Lamdul engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

i. December 4, 2019 - $20,000 wire to Conspirator 13.

37. According to an interview with Person 35, whose identity is known to the affiant, Person 35 met somebody he/she believed to be named Rebecca Owens on Zoosk in the fall 2019. Owens

told Person 35 that she was going to receive an inheritance, and she asked Person 35 to send money to various people and companies to pay for expenses related to shipping the inheritance. Person 35 often sent money and received supposed tracking codes related to the package, but the codes never worked. Person 35 eventually found out, with the help of his/her family, that he/she was being scammed. Bank records show that, on December 13, 2019, an official check purchased by Person 35 in the amount of $60,000 was deposited into BOA xx3392.

a. Bank records show that, after receiving the funds, Lamdul engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

    i. December 20, 2019 - $58,500 wire to Company 9 located in Dublin, Ireland.

38. According to an interview with Person 36, whose identity is known to the affiant, Person 36 met somebody he/she believed to be named Howell Jones on Ourtime in October 2019. Person 36 and Jones communicated via Google Hangouts. Jones told Person 36 he was serving in Afghanistan in the Army, and he needed assistance paying fees associated with a shipment of gold bars. Person 36 sent approximately $500,000 to various people at Jones' request. Person 36 has asked Jones numerous times for repayment, but Jones will not talk to him/her. Bank records show that, on December 26, 2019, Person 36 wired $50,000 to BOA xx3392.

a. Bank records show that, after receiving the funds, Lamdul engaged in the following monetary transaction in criminally derived property of a value greater than $10,000, which was also a financial transaction designed to conceal the nature, source, location, ownership and/or control of the funds:

    i. December 27, 2019 - $50,000 wire to Company 10 in the United Kingdom.

39. According to an interview with Person 46, whose identity is known to the affiant, Person 46 met somebody he/she believed to be named Sharon Wallace in December 2019. Wallace told Person 46 that she had inherited gold worth millions of dollars and needed Person 46's assistance paying fees related to releasing the gold. Person 46 sent funds at Wallace's request, but he later discovered that he had been scammed. Bank records show that Person 46 wired at total of $50,000 to Key xx7278 between February 20, 2020 and February 21, 2020. Memoranda on the wires read, "For Sharon Wallace."

a. Bank records show that, after receiving the funds, Lamdul engaged in the following financial transactions designed to conceal the nature, source, location, ownership and/or control of the funds:

    i. February 21, 2020 - $3,600 cash withdrawal.

ii. February 21, 2020 – purchase of an official check in the amount of $5,000 payable to a third party.

iii. February 21, 2020 – purchase of a second official check in the amount of $5,000 payable to a different third party.

iv. February 24, 2020 – purchase of an official check in the amount of $6,500 payable to a third party.

v. February 24, 2020 - $5,000 cash withdrawal.

vi. February 25, 2020 – purchase of an official check in the amount of $7,000 payable to a third party.

40. Further analysis of the bank records related to the accounts held in the name of Brandtown shows that additional funds characteristic of derivation from romance fraud were deposited and/or wired into the accounts. Not all the individuals from whom funds were received were interviewed. However, deposits from many of the individuals share characteristics with those deposits known to have originated from romance fraud. A summary of the account deposits is included below:

a. Between July 6, 2019 and November 6, 2019, deposits into JPMC xx9549 totaled $422,766.71. Of these deposits, at least $335,736 was characteristic of derivation from romance fraud.

b. Between November 21, 2019 and February 29, 2020, deposits into BOA xx3392 totaled $280,267.42. Of these deposits, at least $234,079.25 was characteristic of derivation from romance fraud.

c. Between February 3, 2020 and May 31, 2020, deposits into Key xx7278 totaled $50,605.76. Of these deposits, $50,000 was characteristic of derivation from romance fraud.

Amankwah and EKA Consulting (EKA)

41. As stated in paragraph # 34, Person 32 provided information indicating that he/she was the victim of a romance scam. Bank records show that, on September 20, 2019, an official check in the amount of $96,000 payable to EKA purchased by Person 32 was deposited into JPMC xx7723.

42. According to an interview with Person 42, whose identity is known to the affiant, Person 42 met somebody he/she believed to be named Wayne Cornelis online sometime in 2019. Cornelis told Person 42 that he was in the Special Forces serving in Iraq, and he had been awarded a reward for saving a man's family. Cornelis put Person 42 in contact with somebody Person 42 believed to be named Peter Tinsley. Tinsley instructed Person 42 to send money to various businesses as payments of taxes, customs fees and other expenses related to the shipment of the

reward. Person 42 never received the reward or any returned funds. Bank records show that between October 16, 2019 and March 24, 2020, Person 42 wired $491,773.57 to JPMC xx7723. Bank records also show that, on November 7, 2019, Person 42 wired $42,145 to BOA xx2925.

43. According to an interview with Person 43, whose identity is known to the affiant, Person 43 met somebody he/she believed to be named Mizway Brian on a dating website sometime in the summer of 2019. Brian told Person 43 that she lived in Richmond, VA, but she used to live with her aunt in Great Britain. Her aunt had married a wealthy British man who had died and left her a fortune. Sometime later, Brian's aunt allegedly died and left Brian an inheritance. The inheritance consisted of gold and diamonds worth $66 million, but the assets were in Great Britain. Person 43 was later contacted by somebody he/she believed to be named Andy Harris. Harris told Person 43 that he was an attorney in Great Britain. Harris further told Person 43 that Brian was not capable of handling the issues related to her inheritance. As such, Harris told Person 43, if Person 43 paid some of the upfront costs associated with the inheritance, he/she would be entitled to part of it. Person 43 never received any portion of the inheritance. Bank records show that between December 3, 2019 and March 4, 2020, Person 43 wired $342,000 into JPMC xx7723 and $17,000 into PNC xx4725.

44. As stated in paragraph # 28, Person 41 provided information indicating that he/she was the victim of a romance scam. Bank records show that, between January 28, 2020 and February 18, 2020, Person 41 wired $827,000 into JPMC xx7723.

45. Further analysis of the bank records related to JPMC xx7723 shows that additional funds characteristic of derivation from romance fraud were deposited and/or wired into the account. Not all the individuals from whom funds were received were interviewed. However, deposits from many of the individuals share characteristics with those deposits known to have originated from romance fraud. Bank records show that deposits into JPMC xx7723 between July 30, 2019 and April 30, 2020 which were characteristic of fraud totaled at least $3,026,265.57. After receiving the funds into JPMC xx7723, Amankwah engaged in the following notable financial transactions designed to conceal the nature, source, location, ownership and/or control of the funds, some of which were monetary transactions in criminally derived property of a value greater than $10,000:

a. Cash withdrawals totaling at least $153,150

b. October 2, 2019 - $85,000 wire to Company 9 in Dublin, Ireland

c. October 18, 2019 - $180,000 wire to Company 9 in Dublin, Ireland

d. November 9, 2019 – $13,700 official check payable to LSG

e. November 12, 2019 - $30,500 wire to Conspirator 13

f. December 2, 2019 - $65,000 wire to Company 9 Dublin, Ireland

g. December 4, 2019 - $134,000 wire to Company 9 in Dublin, Ireland

h. December 10, 2019 - $20,000 wire to Conspirator 13

i. December 24, 2019 - $67,152 wire to Company 10 in the United Kingdom

j. February 18, 2020 - $153,000 wire to a bank account in Hong Kong

k. February 18, 2020 - $30,000 wire to a bank account in Canada

l. February 18, 2020 - $37,000 wire to a bank account in Canada

m. March 10, 2020 - $70,000 wire to Company 5

n. March 27, 2020 - $15,700 wire to Company 5

46. As stated in paragraph # 36, Person 34 provided information indicating he/she was the victim of a romance scam. Bank records show that, on March 3, 2020, Person 34 wired $99,900 to BOA xx2925. Bank records also show that, on March 23, 2020, Person 34 wired $31,500 to PNC xx4725

a. Bank records show that, after receiving the funds, Amankwah engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. March 5, 2020 - $100,000 wire to Company 5 from BOA xx2925.

47. According to an interview with Person 44, whose identity is known to the affiant, Person 44 met somebody he/she believed to be named Maria Christina Batista on Match.com in or around August 2019. Person 44 communicated with Batista via email, WhatsApp and Google Hangouts. Batista told Person 44 she was serving in the military in Kuwait and had inherited $10 million worth of Bitcoin. Batista referred Person 44 to Jamie Simmonas, who was supposed to assist with the inheritance. Person 44 ultimately sent money as requested by Batista and Simmonas to various people and companies to assist Batista with acquiring the inheritance. Person 44 believes he/she sent close to $1 million total. Person 44 has never received any part of the alleged inheritance.

a. Bank records show that, after receiving the funds, Amankwah engaged in the following monetary transaction in criminally derived property of a value greater than $10,000:

i. March 11, 2020 - $30,000 wire to Company 5

48. Further analysis of the bank records related to BOA xx2925 and PNC xx4725 shows that additional funds characteristic of derivation from romance fraud were deposited and/or wired into the accounts. Not all the individuals from whom funds were received were interviewed. However, deposits from many of the individuals share characteristics with those deposits known

to have originated from romance fraud. Bank records show that deposits into BOA xx2925 between October 4, 2019 and March 31, 2020 which were characteristic of fraud totaled at least $1,201,498.03. Bank records show that deposits into PNC xx4725 between February 13, 2020 and March 31, 2020 which were characteristic of fraud totaled at least $64,700.

49. In total, Amankwah received at least $4,292,463 in receipts characteristic of fraud into accounts held in the name of EKA between 2019 and 2020.

Use of Electronic Devices

Prior Cell Phone Searches

50. On March 4, 2020, Asante and two others were arrested following the filing of Criminal Complaints charging them with conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h). When he was arrested, Asante was in possession of two iPhones. IRS-CI applied for and was granted warrants to search both phones. The searches revealed that one of the phone numbers assigned to the phones was 347-446-5619. The searches also revealed that Asante possessed audio files, text messaging application files, and image files relevant to the conspiracy in which he, Wellington, Toure, Lamdul, Amankwah and others were involved. The searches also revealed that it is likely that Wellington, Toure, Lamdul and Amankwah also use their cell phones in furtherance of their criminal activities.

Items Relevant to Wellington

51. One or both of Asante's phones contained five different audio recordings which captured conversations between Wellington and JP Morgan Chase Bank employees. The file names indicate that the recordings were created between November 27, 2018 and December 17, 2018. The content of the recordings indicate that the conversations involved JPMC xx3056 and the funds received from Person 37. The recordings included the following:

a. In one recording, when asked by a JP Morgan Chase employee about the source of the funds, Wellington claimed that the funds originated from her business partner, Person 37. In a different recording, Wellington claimed that Person 37 was an investor. When asked by a JP Morgan Chase employee if she was planning to add Person 37 as a signer on the account, Wellington responded in the affirmative. According to Person 37, he/she was the victim of a romance scam – not Wellington's business partner or an investor.

b. Wellington, at various times in the recordings, stated that she needed the funds for a business that she was running; to ship a container; to buy new merchandise and inventory; to re-up on her products; to travel abroad; and for payroll. Activity in JPMC xx3056 indicates that none of these statements was true.

c. These recordings relate to above-referenced Bank Fraud Conspiracy count with which Asante and Wellington have been charged.

52. One or both of Asante's phones contained various images of business and/or banking information related to Wellington and LSG. One of these images was a screenshot from NFS.us thanking Wellington for using NFS for her business registration. The business registered is shown to be LSG on September 14, 2018. As described in paragraph # 16, Wellington established LSG through National Filing Systems, LLC on September 14, 2018.

53. One or both of Asante's phones contained WhatsApp text messages. I know from investigative experience that WhatsApp is a smart phone application which can also be accessed via a computer. WhatsApp is a free instant messaging and voice over internet protocol service. The user of the application downloads the application to their phone and/or computer, and the application requires the user to assign a phone number to the application. After a phone number is assigned to the application, the application sends a verification text to the phone number assigned. In this way, the application is linked to the phone number of the phone onto which the application was downloaded.

54. I also know that smart phone applications such as WhatsApp are often installed on the phones of the perpetrators of fraud schemes such as this. This application is used by persons engaged in fraud to communicate with individuals while potentially disguising their true identities. These communications can include communications with co-conspirators as well as victims.

55. The WhatsApp text messages included a conversation between Asante and phone number 614-377-8060. The messages showed that this number belonged to "Alexis." Wellington also provided this number to JP Morgan Chase when opening a bank account on November 24, 2018. This indicates that Wellington also uses WhatsApp.

Items Relevant to Toure

56. One or both phones contained WhatsApp text messages showing that in December of 2019, Asante engaged in a WhatsApp conversation with phone number 929-530-0983. The messages showed that this number belonged to "Lamine." Toure's full name is Mohamed Lamine Toure, and Toure provided this same phone number to JP Morgan Chase when he opened bank account # xx8701 in the name of Lamzol in 2019. The conversation consisted of the following excerpt that occurred on December 26, 2019:

> Toure: My boss merry Christmas
>
> Asante: Did dey release de $17500
>
> Toure: No they did not…Did u speak with ur guys?...I feel like we should wait on the client to clear the 400 first cause that's where the problem started.

57. One or both phones contained a recording, which the file name indicates was created on February 25, 2020. The recording captured an approximately 16-minute conversation between Toure and a Bank of America employee. In the conversation, Toure identified himself and said his company was Lamzol. Toure stated that one of his "clientele" had accidentally wired

$400,000 to the account, and the money had been returned to the "client." The bank employee then informed Toure that his account was frozen due to suspicious activity in the account.

58. The timing of the conversation between Toure and Asante and the timing of the conversation between Toure and the Bank of America employee indicate that each likely pertained to the $400,000 received from Person 41.

59. One or both phones contained various images of business and/or banking information related to Toure and Lamzol. Some of these images included the following:

a. An image of a receipt showing a balance inquiry made related to FTB xx8074 on August 8, 2019. The balance in the account on that date was $49,925. As stated in paragraph # 21, $47,325 from Person 38 had been deposited into the account on or about August 5, 2019.

b. An image of a funds transfer request showing a $41,500 wire transfer from BOA xx1870 to Company 11 on August 27, 2019. As stated in paragraph # 25, $47,325 from Person 38 had been deposited into the account on or about August 5, 2019. Toure then wired $41,500 to Company 11 on August 27, 2019.

c. An image of a transaction receipt showing an $11,000 transfer from BOA xx1870 to another Bank of America account on December 17, 2019. As stated in paragraph # 26, Person 39 wired $35,780 to BOA xx1870 on December 16, 2019. Toure then transferred $11,000 to Company 12 on December 17, 2019.

Items Relevant to Lamdul

60. One or both phones contained a recording, which the file name indicates was creating on November 25, 2019. The recording captured an approximately 10-minute conversation between Lamdul and JP Morgan Chase employees. In the conversation, Lamdul identified himself and his business, Brandtown. Lamdul said he believed his account had been closed and asked about a check in the amount of $26,400. Lamdul stated that he believed it was sent back to "the client…the customer that I wired it to." The JP Morgan Chase employee informed Lamdul that a wire in the amount of $26,400 had been recalled. Lamdul asked, "Who was the sender? Because I work with a lot of clients…" The JP Morgan Chase employee informed Lamdul from whom the wire had originated and that the sender had requested a recall of the wire. Lamdul explained to the JP Morgan Chase employee that he was trying to get his money back from them. He further stated that he "works with a lot of people, and it's hard for me to keep track of everybody." Information contained within this affidavit indicates that Lamdul's statements to the JP Morgan Chase employee were false.

61. One or both phones contained a recording, which the file name indicates was also created on November 25, 2019. The recording is likely a continuation of the previous recording. At the end of the recording, a second male voice asks the JP Morgan Chase employee, "Yeah, so when are they going to send the $26,400…because, what I was saying is, if you send it back, how am I going to get my money if I work for the person?"

a. The affiant has listened to Asante speak and has listened to the recording. The affiant believes the second male voice is Asante's voice.

62. One or both phones contained various images of business and/or banking information related to Lamdul and Brandtown. Some of these images included the following:

a. An image of a wire transfer outgoing request showing a $23,800 wire transfer from JPMC xx9579 to Conspirator 12 on September 16, 2019. As stated in paragraph # 33, Person 31 deposited $27,000 cash into JPMC xx9579 on September 12, 2019. Lamdul then wired $23,800 to Conspirator 12 on September 16, 2019.

b. An image of a wire transfer outgoing request showing a $66,000 wire transfer from JPMC xx9579 to Company 9 on September 25, 2019. As stated in paragraph # 34, $75,000 from Person 32 was deposited into JPMC xx9579 on September 23, 2019. Lamdul then wired $66,000 to Company 9 on September 25, 2019.

c. An image of an official check in the amount of $7,000 payable to a third party issued from Key Bank and dated February 25, 2020. As stated in paragraph # 39, Person 46 had wired $50,000 into Key xx7278 between February 20, 2020 and February 21, 2020. Lamdul then purchased various cashier's checks payable to third parties, including one on February 25, 2020 in the amount of $7,000.

63. One or both phones contained WhatsApp text messages between Asante and phone number 614-596-6089. Asante listed this number in his contacts as belonging to "Uriah." A photo associated with the phone number appears to be a picture of Lamdul. The text conversation consisted of the following excerpt that occurred on January 16, 2020:

Asante: I wanted my bro to pick up de 4K. Did de payment clear yet?

Lamdul: Not in the area rn tho, if you can give me a few. And no it's says on the 23rd

Asante: Lol I just saw de date on it. Ok lemme know wat time he could meet u n pick it

Items Relevant to Amankwah

64. One or both phones contained various images of business and/or banking information related to Amankwah and EKA. Some of these images included the following:

a. An image of an official check in the amount of $70,000 payable to EKA purchased by Person 48, as well as an image of a deposit slip showing that $70,000 was deposited into BOA xx2925 on January 21, 2020. Bank records

show that on January 21, 2020, $70,000 from Person 48 was deposited into BOA xx2925.

b. An image of a cell phone showing online banking activity in JPMC xx7723. Bank records show that the image corresponds to activity occurring in JPMC xx7723 on February 18, 2020, including some of the transactions detailed in paragraph #45.

c. A cropped image of a wire confirmation showing that Person 42 had wired $275,362.57 to JPMC xx7723 on October 16, 2019. As detailed in paragraph # 42, bank records show that between October 16, 2019 and March 24, 2020, Person 42 wired a total of $491,773.57 to JPMC xx7723.

65. One or both phones contained WhatsApp text messages between Asante and phone number 614-589-8380. AT&T records show that between at least December 5, 2014 and July 1, 2021, the subscriber to this phone number was Amankwah. The text conversation consisted of the following excerpts:

a. December 24, 2019

Asante: Did u see de message for de payment

Amankwah: Yea there is another coming in

Amankwah then sent two images to Asante. The first image was of a cell phone showing banking activity inside a Bank of America bank account. The second image was of a cell phone showing banking activity inside a JP Morgan Chase bank account. Comparison to BOA xx2925 and JPMC xx7723 shows that the images corresponded to activity in the accounts.

b. January 27, 2019 (10:04)

Asante: Company name: (Company 13) ventures llc…Chase bank

Asante then sent Amankwah an image showing a bank account number and routing number.

c. January 27, 2019 (10:34)

Asante: Pay $5,200 to dis chase account..do it on a computer

Asante then provided Amankwah with the name of Company 14 and bank account information related to Company 14. Asante instructed Amankwah to, "Pay $5,000 into this Account."

Analysis of BOA xx2925 shows that Amankwah transferred $5,000 to Company 14 on January 27, 2019 and $5,200 to Company 13 on January 28, 2019.

d. February 29, 2020

Asante sent Amankwah two images. The first image was of a FedEx express receipt showing that a package had been sent to EKA located at 5390 Cambria Way, Westerville, OH from Bakersfield, CA. The next image was of an official check in the amount of $25,000 payable to EKA purchased by Person 47.

Analysis of JPMC xx7723 shows that $25,000 from Person 47 was deposited into the account on or about March 10, 2020.

Toll Records

66. T-Mobile records show that Wellington was the subscriber to phone number 614-377-8060 from November 8, 2011 through November 27, 2019, and from November 27, 2019 through at least July 12, 2021 Asante was the subscriber. Various sources of information obtained during the investigation indicate that Asante and Wellington are romantically involved. As such, the subscriber change may be related to Asante simply assuming financial responsibility for the line. The records further show that 614-377-8060 and 347-446-5619, Asante's phone number, placed or received calls from one another at least 879 times between July 9, 2019 and May 10, 2021.

67. AT&T records show that phone number 614-589-8380 placed or received calls from 347-446-5619 at least 125 times between October 27, 2018 and May 15, 2020. As stated in paragraph # 65, Amankwah is the subscriber to phone number 614-589-8380.

Pen Register and Trap and Trace

68. Between September 20, 2019 and November 14, 2019, IRS-CI placed Pen Register and Trap and Trace devices on various WhatsApp phone numbers, including 347-446-5619, Asante's phone number. The Pen Register and Trap and Trace devices revealed that:

a. 347-446-5619 placed or received calls and/or messages from 614-377-8060 at least 894 times during the time period captured. As stated in paragraphs # 55 and # 66, this number is believed to belong to Wellington.

b. 347-446-5619 placed or received calls and/or messages from 614-596-6089 at least 237 times during the time period captured. As stated in paragraph #63, this number is believed to belong to Lamdul.

c. 347-446-5619 placed or received calls and/or messages from 614-589-8380 at least 117 times during the time period captured. As stated in paragraph # 65, Amankwah was the subscriber to 614-589-8380.

69. The WhatsApp communications captured by the Pen Register and Trap and Trace devices would not be recorded in toll records because they were facilitated through the WhatsApp application.

70. The Pen Register and Trap and Trace device results revealed that the phones being used by Wellington and Lamdul to send outgoing messages via WhatsApp were iPhones while the device being used by Amankwah was an Android device. Samsung phones function on the Android operating system.

Technical Background

71. Based upon my training and experience, I use the following technical terms to convey the following meanings:

a. Cell Phone/Mobile Device: A cell phone is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

72. Based upon my training, experience and research, I know that the devices for which the warrants are requested have capabilities to allow them to serve as a cell phone, digital camera, portable media player, GPS navigation device and PDA.

73. I have consulted with IRS-CI Special Agent-Computer Investigative Specialist Ebenger-Balla regarding the aspects of properly retrieving and analyzing electronically stored digital data. Special Agent Ebenger-Balla has been employed with IRS-CI since 2009. In addition to attending training in financial investigation techniques and accounting, she also completed the IRS-CI Basic Computer Evidence Recovery Training class at the Federal Law Enforcement Training Center in Glynco, Georgia, (2016) and the Advanced Computer Evidence Recovery Training class at the CyberCrimes Center in Fairfax, Virginia (2017), and Macintosh Forensics Training in Glynco, Georgia (2017). Special Agent Ebenger-Balla also completed the Mobile Device Forensics Training in Glynco, Georgia (2017) where she learned about the operation of mobile devices and the correct procedures for seizing and analyzing those devices.

74. Based upon the affiant's knowledge, training, experience and consultation with Special Agent Ebenger-Balla, the affiant knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for

some period of time on the device. This information can sometimes be recovered with forensic tools.

75. As further described in Attachments E, F, G and H, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium

76. The affiant knows that searching and seizing information from computers and cell phones often requires agents to seize most or all electronic storage devices to be imaged and searched later by a qualified computer specialist in a laboratory or other controlled environment. This requirement is due to the following:

a. Technical requirements: Searching computer systems, such as cell phones, for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. Data search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or

destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis. Further, such searches often require the seizure of most or all of a computer system's input/output peripheral devices, related software, documentation, and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment.

b. The volume and nature of electronic evidence: The volume of evidence. Computer storage devices such as cell phones can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

77. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

Conclusion

78. Based on the information presented in this affidavit, I contend that Wellington, Toure, Lamdul, Amankwah and others were engaged in a conspiracy to commit money laundering in violation of 18 U.S.C. § 1956(h). I further contend that Wellington, Lamdul, Toure, Amankwah and others each personally committed multiple acts in violation of 18 U.S.C. § 1956(a)(1)(B)(i) and/or 18 U.S.C. § 1957 in furtherance of the conspiracy. I further believe that Wellington, Lamdul, Toure, Amankwah and others used various electronic devices, namely their cell phones, to communicate regarding and to facilitate the laundering of funds derived from fraud schemes, and evidence of these violations, as well as violations of 18 U.S.C. § 1343, is now located in the items described in Attachments A, B, C and D. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

Shawn A. Mincks
Special Agent, IRS-CI

Subscribed and sworn to before me

This 2nd day of August, 2021.

THE HONORABLE ELIZABETH A. PRESTON DEAVERS
United States Magistrate Judge

UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO

ATTACHMENT B

The property to be searched is a black and gray iPhone cell phone seized during the arrest of Mohamed Toure on July 26, 2021.

Hereinafter this cellular telephone will be referred to as the "Device." The Device is currently located at 401 N. Front Street, Suite 375, Columbus, Ohio.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment F.

ATTACHMENT F

1. All records on the Device described in Attachment B that are evidence of violations of 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1349 (conspiracy to commit bank fraud); any section of 18 U.S.C. § 1956 (money laundering) and/or 18 U.S.C. § 1957 (money laundering), for the period October 1, 2018 to the present, including:

   a. Records identifying the establishment, ownership, operation and/or control of any limited liability corporation or other business entity including articles of organization; correspondence with and/or submissions to/from any Secretary of State office; applications, disposition records and/or correspondence related to the issuance or use of Employer Identification Numbers (EIN); minutes and other official business records; and documents identifying any registered agent(s), incorporator(s), and/or other identified members;

   b. All records related to or referencing electronic transfers of funds or cash deposits including requests for an electronic transfer or cash deposit, wiring or deposit instructions, receipts, and correspondence;

   c. All records related or referring to persons or entities in other countries and the locations of such persons or entities;

   d. Asset ownership and/or acquisition records including contracts, invoices, receipts, registrations, titles insurance records and/or photographs of assets including motor vehicles, real property, boats, jewelry, precious metals and gems, and currency (foreign, domestic, or virtual currency);

   e. Travel records including travel directions, hotel reservations, rental car reservations, airplane reservations, invoices, airline tickets, and itineraries;

   f. Records related to banking activity including communications and data related to the opening, closing, use, custody and/or control of bank accounts, alternative currency accounts (i.e. those related to Bitcoins), credit cards, and/or debit cards including applications for accounts; approval or declination notices; credit and/or debit card issuance notices; credit and/or debit card activations; bank statements; welcome or account opening/closing notifications; deposit, payment, withdrawal, or transfer orders, receipts and/or notifications; balance inquiries and/or notices; and security notifications;

   g. All financial statements, accounting records and supporting source documents relating to receipts, expenditures, general ledgers, accounts and notes receivable, accounts and notes payable, balance sheets, income statements, statements of profit and loss, and any other accounting records and other records and/or ledgers relating to Lexis Solutions Group, Ingwet Canal, Brandtown Logistics, Lamzol Trucking & Logistics, EKA Consulting or any variation of these entity names or any other entities

identified through items seized pursuant to section a. above;

h. Records pertaining to any financial institution account including but not limited to account numbers, passwords, personal identification numbers (PINS), deposit/withdrawal records, notes, logs, and photographs;

i. Electronic records of internet sites visited and data accessed and/or communications made in the course of visiting such internet sites;

j. Communications records and histories made through and/or from applications (known as "Apps"); emails; texts; calls or other media contained on the electronic devices to be searched and all attachments included in such communications; and

k. Contact lists and any documents reflecting names, addresses, email addresses, telephone numbers, fax numbers and/or other contact information.

2. Evidence of user attribution showing who used or owned the cell phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.